Remarks/Arguments

Claims 1-50 remain in this application. Claim 44 has been amended to delete the word "have" on line 3 to replace it with "having" in order to correct the tense of the verb.

The Examiner has rejected Claims 1-30 and 32-38 as being anticipated by Vanstone et al. (U.S. Patent No. 6,446,207).

Claim 1 recites "A method of verifying a transaction over a data communication system between a first and a second correspondent through the use of a certifying authority".

Claim 1 recites steps performed by the certifying authority, steps b) and c), relating to generating implicit signature components, and then, at steps d) and e), forwarding at least one of the implicit signature components to each of the correspondents. No such steps are disclosed by the reference to Vanstone et al.

Claim 1 further recites the steps of one of the correspondents signing a message with an ephemeral private key at step f) and forwarding the message to the other correspondent, which verifies the signature using a corresponding ephemeral public key. Thus, Claim 1 discloses a five-pass verification protocol, wherein the recipient of a message requests transaction specific information, in the form of components of an implicit certificate, from the certifying authority. The recipient passes this information to the sender, who then computes a transaction-specific private key, signs the message and sends the message along to the recipient. Finally, the recipient verifies the signature using the sender's public key computed from the information provided by the certifying authority.

The reference to Vanstone et al. discloses a one-pass verification protocol where both correspondents share a private key (column 3, lines 18 to 22). The present application does not require the correspondents to have a shared private key but rather depends upon the recipient generating the sender's public key. As may be clearly seen, the reference to Vanstone et al. does

not teach of a five-pass protocol involving two correspondents and a certifying authority, wherein the recipient requests components of an implicit certificate from the certifying authority for every signed transaction.

Accordingly, it is believed that Claim 1 presently on file clearly and patentably distinguishes over the Vanstone et al. reference and as such is in condition for allowance. Furthermore, Claims 2-30 and 32-38 presently on file being dependent upon Claim 1, it is believed they also clearly and patentably distinguish over the Vanstone et al. reference.

The Examiner has rejected Claims 31, 39, and 44-50 as being unpatentable over Vanstone et al. and further in view of Perlman et al. (U.S. Patent No. 6, 230,266).

Claim 44 recites "a method for certifying a correspondent through the use of a certifying authority having control of a certificate's validity", "wherein said certifying authority rectifies said correspondent's certificate by changing said value of said first random number". The Examiner has noted that Vanstone et al. "fails to disclose the CA rectifying the certificate", the Examiner also comments that Perlman et al. "teaches an authentication method to efficiently and securely re-establish authentication system security after a detection of a compromise of one of the online line revocation servers (OLRS) by rectifying the certificate without discontinuing the original certification and issuing new certificates (col.3, lines 22-53)".

The Applicant submits that Perlman et al. more specifically teaches that "If the CA is treated as if it has been compromised, in order to re-establish authentication system security, it becomes necessary to (1) discontinue use of the current CA and OLRS, (2) begin using a new CA and OLRS, each of which have new respective private/public key pairs that are different from those used by the CA and OLRS that are no longer being used, (3) notify all other certificate authorities that previously issued certificates for the current CA's public key that such certificates should now be revoked, and (4) issue new certificates signed by the private key of the new CA that rectify principals' valid public keys that has been previously certified by the CA whose use is being discontinued." (col.3, lines 41-53). Perlman et al. teaches the use of

redundant CAs and revocation servers to prevent recertifying the entire trust network should the primary CA be compromised, thus Perlman et al. teaches a method to avoid recertifying keys, which teaches away from the methods recited by Claim 44, which teaches recertifying keys on every transaction with a single CA.

Accordingly, it is believed that Claim 44 as amended clearly and patentably distinguishes over the Vanstone et al. reference in view of the Perlman et al. reference and as such is in condition for allowance. Furthermore, Claims 45-50 presently on file being dependent upon Claim 44, it is believed they also clearly and patentably distinguish over the Vanstone et al. reference in view of the Perlman et al. reference.

As for Claims 31 and 39, as per the arguments for Claim 1 combined with the arguments of Claim 44, i.e. that the Perlman et al. reference does not teach rectification of keys on every transaction with a single CA, it is also believed that Claims 31 and 39 presently on file, being dependent upon Claim 1, also clearly and patentably distinguish over the Vanstone et al. reference in view of the Perlman et al. reference.

Further consideration to allowances respectfully requested.

Respectfully submitted,

John R.S. Orange
Agent for Applicant
Registration No. 29,725

Date: March 5, 2004

McCarthy Tetrault LLP
P.O. Box 48, Suite 4700, Toronto Dominion Bank Tower
66 Wellington St. West
Toronto, Ontario M5K 1E6, Canada

Tel: (416) 362-1812

JRO/CR/sp